

## **Sample: f4114b3006806d7ee27af23978591fbb**

P3pper Reports - <http://www.peppermalware.com>.

P3pper Twitter - <https://twitter.com/P3pperP0tts>.

This report has been generated automatically by a set of malware analysis tools.

This work is licensed under a Creative Commons Attribution 4.0 International License. To view a copy of this license visit <http://creativecommons.org/licenses/by/4.0/>.

Classification: **#BANKER #BLACKMOON** (based on p3pperp0tts rules)

Analysis date: 2019-03-11 03:13:29 (p3pperp0tts platform's analysis date)

Exe timestamp: 2016-05-04 10:28:09 (timestamp of the original sample)

Unpacked mods max timestamp: 2016-05-04 10:28:09 (higher timestamp of all the unpacked modules)

VirusTotal analysis date: 2019-03-04 03:30:32 (date of last time that the sample was analyzed at vt)

### **Index**

- [Sample](#)
- [AV detections](#)
- [Source](#)
- [Virustotal](#)
- [Threads tree](#)
- [Most Interesting behavior](#)
- [Most Interesting strings](#)
- [Hosts](#)
- [Dns queries](#)
- [Network traffic](#)
- [Full strings list](#)
- [Threads behaviour](#)
- [Network by processes](#)
- [Unpacked or injected modules](#)
- [Extra Information Recovered](#)
- [Configs Recovered](#)

## Sample

•md5: f4114b3006806d7ee27af23978591fbb

## AV detections

- Microsoft: TrojanSpy:Win32/Banker
- Kaspersky: HEUR:Trojan.Win32.Generic
- Symantec: Trojan.Gen.2
- Malwarebytes: Spyware.PasswordStealer

## Source

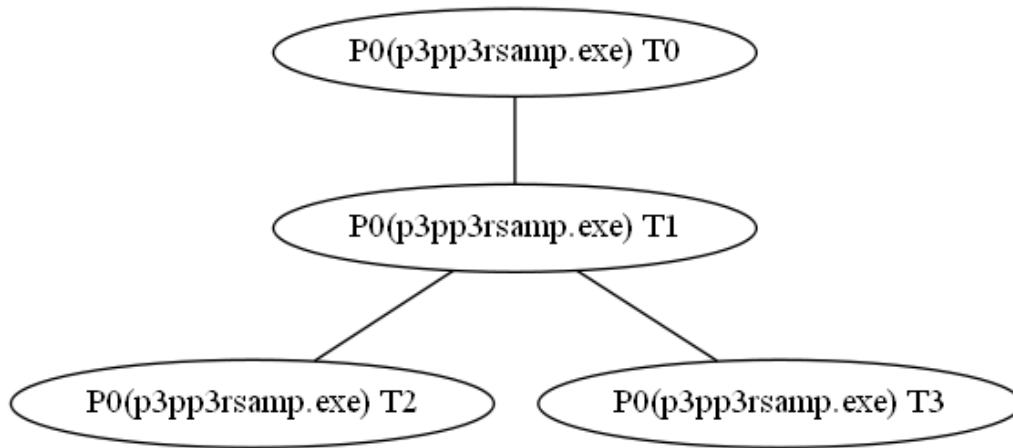
•

## Virustotal

- <https://virustotal.com/es/file/80ea86d195bbc4384a1b9a77a2d477e2c4e6dc6d48f3f80447877dbbe41a4e40/analysis>

## Threads tree

The following tree represents sample's threads. T<index> is an alias for sample's threads (numeration is done in the order of threads creation). P<index> is an alias for processes owning sample's threads.



## Most interesting behavior

The following list is a collection of the most interesting events captured. This list is ordered by the score assigned to the event. In the section "Threads behavioural information" it's possible to find all the actions performed by each sample's thread ordered chronologically.

- RegCreateKey (HKCU\\Software\\Microsoft\\Windows Script\\Settings Desired Access: Maximum Allowed, Granted Access: All Access, Disposition: REG\_OPENED\_EXISTING\_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG\_OPENED\_EXISTING\_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG\_OPENED\_EXISTING\_KEY)
- RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run Desired Access: Read/Write, Disposition: REG\_OPENED\_EXISTING\_KEY)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\000C29FC2AB3 Type: REG\_SZ, Length: 82, Data: C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe)
- Thread Create ( Thread ID: T1)
- Thread Create ( Thread ID: TUNKALIAS)
- Thread Create ( Thread ID: T2)
- Thread Create ( Thread ID: T3)

## Most interesting strings

The following list is a collection of the most interesting strings found in the sample's modules (unpacked modules too) code or data.

- <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
- !This program cannot be run in DOS mode.
- <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
- <requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
- PathFileExistsA
- InternalName
- 997A9EB2E9701AB8476AD6E56E12C8C93CF
- cracked by ximo
- </requestedPrivileges>
- Copyright 2016 Veurtotcm Appile Incorporated. All rights reserved.
- LegalCopyright
- OriginalFilename
- GetProcAddress
- cracked by ximot
- </trustInfo>
- VS\_VERSION\_INFO
- The procedure entry point %s could not be located in the dynamic link library %s
- VURinstallecoder.dll
- <requestedPrivileges>
- StringFileInfo
- Veurtotcm Appile Incorporated
- (@30D9394BACAEC38335E4EB9DF0AEB7573831B218DEC9A2E26A7113DA3E21A899E7D4E6BE77F87A99B7940F34A157D5DD203EC3FAEF3E9B9610B0009F4F20242B779946334289582B59EA022FE2FC16FE8A8541A6FDCDECFB6EE393B142530B0C803496AAA97F1B7A411D611C205958790C06B8CA87B489AA3A4352B392FAE
- Veuro Quener Xewroxm 2.0
- Build Number
- The ordinal %u could not be located in the dynamic link library %s
- VURinstall Fuerkler
- LOADER ERROR
- >3\$)boxuV[LAal{vUXOB
- Ycracked by ximo
- program internal error number is %d.
- }sqwukiomcage
- Gcracked by ximo
- -&;0YRODu~ch
- GetNativeSystemInfo
- RunTime Error:
- 7:- m`wzYTCN
- CreateThread
- 'cracked by ximo9
- TranslateMessage
- 86\$\*p~lbHFTZ
- cracked by ximoJ
- ;9?=3175+)/-#!'[Y\_]SQWUKIOMCAGE{y
- GetLogicalDriveStringsA
- cracked by ximo4Q
- 3"cracked by ximo
- 2?({nctyZW@M
- cracked by ximo;
- Wow64DisableWow64FsRedirection
- WideCharToMultiByte

- Wow64RevertWow64FsRedirection
- GetModuleHandleA
- RegDisableReflectionKey
- RegEnableReflectionKey
- GetModuleFileNameA
- GetModuleFileNameW
- ConvertSidToStringSidW
- LoadLibraryA
- RtlMoveMemory
- RtlAllocateHeap
- LeaveCriticalSection
- RegQueryValueExA
- GetSystemWow64DirectoryA
- EnterCriticalSection
- RegSetValueExA
- RegCreateKeyExA
- CreateMutexA
- GetEnvironmentVariableA
- RegOpenKeyExA
- InitializeCriticalSection
- GetUserNameA
- GetTempPathA
- DispatchMessageA
- DeleteCriticalSection
- LookupAccountNameA
- WaitForSingleObject
- ReleaseMutex

## Hosts

- 203.205.151.50:http
- google-public-dns-a.google.com:domain
- 192.168.149.166:49159
- 203.205.151.50:80 (users.qzone.qq.com)

## Dns queries

- isatap.localdomain ---> no answers
- users.qzone.qq.com ---> 203.205.151.50
- 8.8.8.8.in-addr.arpa ---> no answers
- 50.151.205.203.in-addr.arpa ---> no answers



## Network traffic

This section contains the readable content of the captured network traffic classified by established connections.

- **tcp 192.168.149.166:49159 ---> 203.205.151.50 (users.qzone.qq.com) :80**

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101  
Safari/537.36[...]Host: users.qzone.qq.com[...]Connection: Keep-Alive[...]GET  
/fcg-bin/cgi_get_portrait.fcg?uins=1960023441 HTTP/1.1
```

- **tcp 203.205.151.50 (users.qzone.qq.com) :80 ---> 192.168.149.166:49159**

```
<center><h1>301 Moved Permanently</h1></center>[...]Location:  
https://users.qzone.qq.com/fcg-bin/cgi_get_portrait.fcg?uins=1960023441[...]Date: Mon, 11 Mar 2019 01:59:00  
GMT[...]Content-Type: text/html[...]<hr><center>stgw/1.3.6.2_1.13.5</center>[...]Content-Length: 192[...]Server:  
stgw/1.3.6.2_1.13.5[...]HTTP/1.1 301 Moved Permanently[...]Connection: Keep-Alive[...]<body  
bgcolor="white">[...]<head><title>301 Moved Permanently</title></head>
```

## Full strings list

The following list it's a collection of all the strings found in the sample's modules (unpacked modules too) code or data.

- <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
- !This program cannot be run in DOS mode.
- <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
- <requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
- PathFileExistsA
- InternalName
- 997A9EB2E9701AB8476AD6E56E12C8C93CF
- cracked by ximo
- </requestedPrivileges>
- Copyright 2016 Veurtotcm Appile Incorporated. All rights reserved.
- LegalCopyright
- OriginalFilename
- GetProcAddress
- cracked by ximot
- </trustInfo>
- VS\_VERSION\_INFO
- The procedure entry point %s could not be located in the dynamic link library %s
- VURinstallecoder.dll
- <requestedPrivileges>
- StringFileInfo
- Veurtotcm Appile Incorporated
- (@30D9394BACAEC38335E4EB9DF0AEB7573831B218DEC9A2E26A7113DA3E21A899E7D4E6BE77F87A99B7940F34A157D5DD203EC3FAEF3E9B9610B0009F4F20242B779946334289582B59EA022FE2FC16FE8A8541A6FDCDECFB6EE393B142530B0C803496AAA97F1B7A411D611C205958790C06B8CA87B489AA3A4352B392FAE
- Veuro Quener Xewroxm 2.0
- Build Number
- The ordinal %u could not be located in the dynamic link library %s
- VURinstall Fuerkler
- LOADER ERROR
- >3\$)boxuV[LAal{vUXOB
- Ycracked by ximo
- program internal error number is %d.
- }sqwukiomcage
- Gcracked by ximo
- -&;0YRODu~ch
- GetNativeSystemInfo
- RunTime Error:
- 7:- m`wzYTCN
- CreateThread
- 'cracked by ximo9
- TranslateMessage
- 86\$\*p~lbHFTZ
- cracked by ximoJ
- ;9?=3175+)/-#!'[Y\_]SQWUKIOMCAGE{y
- GetLogicalDriveStringsA
- cracked by ximo4Q
- 3"cracked by ximo
- 2?({nctyZW@M
- cracked by ximo;
- Wow64DisableWow64FsRedirection
- WideCharToMultiByte

- Wow64RevertWow64FsRedirection
- GetModuleHandleA
- RegDisableReflectionKey
- RegEnableReflectionKey
- GetModuleFileNameA
- GetModuleFileNameW
- ConvertSidToStringSidW
- LoadLibraryA
- 000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F
- 68C5A4A97F0FFA59AA77E0ED3D5CCE4B
- 69C9DFDE7A79FF5C
- 6BB1A5AC7F04F927A802E0913D2DCF323DC48C7BDF0E747A9E73DB32B4F60EEACA56CFB7A3125B552AF3110F587694A8E348E5E5B49FF1B2B568619D60E18C82A6EE55CB
- b5ADVAPI32.dll
- 89BDD449396166926A226D64B4
- 6FC6A4DC780C
- 9125D3B360E98D05F2856630D83630AA
- 23JUSER32.dll
- 68B5DFAD7A05FE27AF02E0E83D58CE3239C7880CDC78747C9B7CDE47B4810E9FC850B5BDA36F5F222FFA1075587D90A29E30E19BC8E2F1C1B66962E965E0F6FDDCE855CD08833D8CB70F345C09E5
- 6EB6A4A0780C
- 6EC9DFAF7D0CFF5C
- 6EC7A4DA7C7AFE29AB0CE19F3A2A
- 69B1A4AB7C7AFA2EAA0DE1913F58CE3A3DC4890ADF0C747D9F7F
- 68B6A5AD7F0FFA5DAA70E09C3D2DCE3B39B18A03A70F720A9D72DE42B4800F94CB21B4B9A4125A552EFC15755E0497AA9F30E090C8EEF5B3B560669F6191F68ADC9956B6768C39FECC01315F08911C6F8FC3D62F18485FBB0FB0C7AD8B4001588666652A3109202C1205F3F9F32C66A1AA179946E7A344A3161BACEF754F9D0
- 69B1A4DE7F7EF95CAA71E0ED3A5BCE4B38C68A03DC78740A9E08DE32B5850E99CB20B4BEA2665C542AFB1071587790A29941E0E5C99EF5B3B36865EB649DF68BDC9951B90B833EF8CD7437290C921F1E8FC8AD5E1F4B5EC90FB6C3A28A43055FFF62675F310C2023
- 6EC9DFA07A05FF5CA80DE49A415ACA3B3AB28E03DA7D727A9F7CDF47B5800B9CCF26B4BFA4125E212988100F5C7C90DA9E45E096C8EDF1B6B163659D649C8D89DC9550CD0B8B4088CA72375C0CE71F628FC8D52C1C4B5EC90FC1C2D48D30062C8162672E310E20231300F7F7F02962DAD71C9B47E7D446A0101EAAE975419A7
- SHGetSpecialFolderPathA
- CoInitialize
- 31AB4231AED9C1F533E7EE7F0A7CB2B3D40B61AA4B9D8956D7F10D43F20A99CE2D5E7B477FD7EEDB096723CDD56D4A72039C2F9EE4BE7ED10C3009D4B5C242770933B3F42FD5F565C9C065EE2FC6D898BF33CA7F8CEE8FC6A9892B03E260C08803596DDA97F1B0C421A60615A56587D0D72C3CF82B6F4D13B4357C1958AEF9
- 69B6DFAA7A79FA5DAA76E09C3A5DCF48
- 6EC6A4AB7F0EF95BAB03E49B3A5DCE3D3EB1
- 6AC1A5AC7C05F927AE07E49A402D
- advapi32.dll
- 6EC7A4AB7F0EFA2AAF03E0ED3A28CF3D
- 69B2A5AD7F0F
- U09GVFdBkUvTWl jcm9zb2Z0XFdpbmRvd3NcQ3VycmVudFZlcnNpb25cUnVuXA==
- FileDescription
- 6AC5A4A97F0AF959AB04
- 68C3DCAB7F79F95EAB04E1EA3A26
- @6AB6A5AD7F0FFA5DAA70E09C3D2DCE3B39B18802DC0F74799E0FDE34C9F50A9FCA54B4BCA3145F5F2E8E100F597695D9E342E4E2B39F
- 6BB5A5AF7C7DFE29AB03E0ED3A5FCE4B3EB78C7BDC0D747D9F7E
- .com6EC7A4DA7C7A
- 68B4A4A97C05FA5BAE07E4EA
- oleaut32.dll
- 68B3A5A07F04FA5DAA77E1913D27CD493EB5880FDF0A74089F7EDE41B4F30FE9
- kernel32.dll
- N@6BB3A5AB7F04F95EAA75E49B3A5ACF3F3DC5887BDC0B0F7C9E72DF45C9F30E95CB50B5B7

- ProductVersion
- 7ac13b3aa82136afa3090c5137
- 6FC9D9DD7878FE29AE0DE49B415D
- 68C4DFA97D79F826AB70E0913A5BCE4B3EB0890D
- 6EB5DEDA7C7EFA26AA76E4EA3A26CB4E39B18D03D80E720F9F72DF42B4870A98CA26B5BBA4115F5E2A891504587C91DE9E48E4E2B19EF1B2B66966996195F1FDDDE954CB0F8F398ACB00305F09911A6C8ACDD6501C4D5EC90ECDC3A28D30055F8666625C36002750
- 68B5DFAD7A05
- RtlMoveMemory
- RtlAllocateHeap
- LeaveCriticalSection
- RegQueryValueExA
- GetSystemWow64DirectoryA
- EnterCriticalSection
- RegSetValueExA
- RegCreateKeyExA
- CreateMutexA
- GetEnvironmentVariableA
- RegOpenKeyExA
- InitializeCriticalSection
- GetUserNameA
- GetTempPathA
- DispatchMessageA
- DeleteCriticalSection
- LookupAccountNameA
- WaitForSingleObject
- ReleaseMutex
- 69B1A5AD7F7AFE27AA76E1903D2CCA3D3FB7897EA60874739F7FDA46CFFC0A9ACF26CEB8A4635D242A8D11005C7293A2E246E694B5E9F5B3B114629C619DF3FDDCEA51BF0FF93D83B602355008911A1A8BB9AC511D4A5FC80FB6C3A48D420329851B672D310E20251304F7F2F42A63AAD7169B43E7A343AD176BAC9E75359A0
- 85" /di~sP]JG
- 6BB2A4AD7F7DF95DAA72E1EC4158CB4E39B18C78DF0D0F729E79DE34B5FD0EEFCB53B5BEA4115A532A8A11005807
- 68B1A4DE7F0FFA29A904E091
- 69C9A5AA7F0EF92FAA04E29C3D26
- 6BB2A4AD7C79F927AB02E09B3A58CE4B3FB78878DC0A737B
- \$-6?HAZS1e~w
- 69B1A4AD7F0FFA5C
- 6BC3A4A17C78
- CoUninitialize
- 68C8A4AC7F05F85DAB02E0913D27
- AO]Sywek1?~#
- [yz;8=>74l2# %&/,)\*
- 69B1A4DE7F7EF95CAA71E0ED3A5BCE4B38C68A03DC78740A9E08DE32B5850E99CB20B4BEA2665D232AFC1102587691AF9E48E19AB2EFF3B0B668659E64E4F682DC9851BF0AFB3DF9B603345C0CE11F638FC8AD5E1E385FC30ECCC2A58A4501288565665A350B25251205F085F32C62A0D7609A46E6D241A1146EABED72469A7
- 68C5A4A17F0FFA5B
- 68C8A5A87C78FA2BAB04E0EF3D5ACF483DC38878DC79730A9C7FDF37B4F40FEDCB20B5B6A36E5F5F2EFB1171580791AC9C43E297C8ECF3C3B61466996593F3F9DC9F51BF0B8E
- @68B1A5AA7F04FA26AA70E0903F2DCE4E3DC0880BDC0D730F9B7BDA40CC850E95CA5DB5CAA4135F222AFC1102587595AE9F49E090C8EFF1B6B41565EC64E7F183DCEA50B60D893DF8B772355A0CEB1E688BBFD15B183D5DCE0FC7C3A08A3503598516672B310F20231302F781F42A61DBD6119A35E6D143A0126DD7E408409D
- MCQ\_u{ig=3! /
- 000C29FC2AB3
- 6AC1A5AC7C05F927AE07E49A402DCB4F3AB78D09D8790E729B7DDB46C9F30BEECE55
- 68B3A5AA7C7AFA28AA76
- 68C6A5A87F04FA29
- 69B5A4A17F0FF82FAA70E1913A5DCA3B38CD887EDC79727A9E0EDF42B5FD0D94CB21B4BBA46F5E21298F10715C7C94DEE241E5E1

- 68C1DCAC7A05FF27AF02E5ED402CCB4F39B18D0CDB0E0E729B73DC32CFF6089BCD55CEBBA3125E5E2A891075597695AD9C32E0E1C8EDF1B4B568659F60978DF8DC9451CB08823DF9B60233290AE21D6F8FC9D55C1D4C5FC80FC6C3A4F631045B8610665E310E5A2C6F00F085F02D61A1D6119E37E6D144A1166EAC9E75359C7
- &=QY.XbN5\$g@Nj
- |ungXQJC4=&/
- zq1gV]@K" )4?
- .' <5BKPfot}
- [X]^WTQRC@EFOLIJKhmngdabspuv
- {pmfW\AJ#(5>
- 4: (&|r`nDJXV79+%`

## Threads behaviour

In this section it's possible to find information about sample's threads, such as the actions performed by each sample's thread ordered chronologically.

- **Thread T0 (in process P0, p3pp3rsamp.exe) description**

- **Thread's childs**

- Thread T1 (in process P0, p3pp3rsamp.exe)

- **Thread' events**

- Thread Create ( Thread ID: T1)

- **Thread T1 (in process P0, p3pp3rsamp.exe) description**

- **Thread's childs**

- Thread T2 (in process P0, p3pp3rsamp.exe)
- Thread T3 (in process P0, p3pp3rsamp.exe)

- **Thread' events**

- Thread Create ( Thread ID: TUNKALIAS)
- RegCreateKey (HKCU\\Software\\Microsoft\\Windows Script\\Settings Desired Access: Maximum Allowed, Granted Access: All Access, Disposition: REG\_OPENED\_EXISTING\_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Query Value, Set Value, Disposition: REG\_OPENED\_EXISTING\_KEY)
- RegCreateKey (HKLM\\Software\\Microsoft\\WBEM\\CIMOM Desired Access: Read/Write, Disposition: REG\_OPENED\_EXISTING\_KEY)
- Thread Create ( Thread ID: T2)
- Thread Create ( Thread ID: T3)
- Thread Create ( Thread ID: TUNKALIAS)
- Thread Create ( Thread ID: TUNKALIAS)
- RegCreateKey (HKCU\\Software\\Microsoft\\Windows Script\\Settings Desired Access: Maximum Allowed, Granted Access: All Access, Disposition: REG\_OPENED\_EXISTING\_KEY)
- RegCreateKey (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run Desired Access: Read/Write, Disposition: REG\_OPENED\_EXISTING\_KEY)
- RegSetValue (HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\000C29FC2AB3 Type: REG\_SZ, Length: 82, Data: C:\\Users\\p3pp3r\\Downloads\\p3pp3rsamp.exe)
- Thread Create ( Thread ID: TUNKALIAS)
- RegCreateKey (HKCU\\Software\\Microsoft\\Windows Script\\Settings Desired Access: Maximum Allowed, Granted Access: All Access, Disposition: REG\_OPENED\_EXISTING\_KEY)

- **Thread T2 (in process P0, p3pp3rsamp.exe) description**

- **Thread's childs**

- No childs found

- **Thread' events**

- Thread Create ( Thread ID: TUNKALIAS)

- **Thread T3 (in process P0, p3pp3rsamp.exe) description**

- **Thread's childs**

- No childs found

- **Thread' events**

- Thread Create ( Thread ID: TUNKALIAS)

- Thread Create ( Thread ID: TUNKALIAS)

## Network by processes

The analysis environment tries to capture and collect network actions performed by sample's threads.

### Process P0 (p3pp3rsamp.exe)'s network events

- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Send (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (36))
- UDP Receive (P3PP3R-PC.localdomain:dynport-> google-public-dns-a.google.com:domain (486))
- TCP Connect (P3PP3R-PC.localdomain:dynport-> 203.205.151.50:http (0))
- TCP Send (P3PP3R-PC.localdomain:dynport-> 203.205.151.50:http (251))
- TCP Receive (P3PP3R-PC.localdomain:dynport-> 203.205.151.50:http (445))
- TCP Disconnect (P3PP3R-PC.localdomain:dynport-> 203.205.151.50:http (0))



## Unpacked or injected modules

In this section it's possible to find information about sample's modules, such as the rich signatures and strings

- **Module 1 (probably unpacked / injected by the sample)**

- **Module 1 rich signatures**

- 44616e53000000000000000000000000007b1c0c0001000000c30f5f000400000831c0e00010000006f1f04000200000036260b000100000036260a0002000000c30f5d0015000000000010089000000000000001000000e81f0b00

- **Module 1 strings**

- **Module 1 most interesting strings**

- <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
- !This program cannot be run in DOS mode.
- <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
- <requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
- PathFileExistsA
- InternalName
- 997A9EB2E9701AB8476AD6E56E12C8C93CF
- cracked by ximo
- </requestedPrivileges>
- Copyright 2016 Veurtotcm Appile Incorporated. All rights reserved.
- LegalCopyright
- OriginalFilename
- GetProcAddress
- cracked by ximot
- </trustInfo>
- VS\_VERSION\_INFO
- The procedure entry point %s could not be located in the dynamic link library %s
- VURinstallecoder.dll
- <requestedPrivileges>
- StringFileInfo
- Veurtotcm Appile Incorporated
- (@30D9394BACAEC38335E4EB9DF0AEB7573831B218DEC9A2E26A7113DA3E21A899E7D4E6BE77F87A99B7940F34A157D5DD203EC3FAEF3E9B9610B0009F4F20242B779946334289582B59EA022FE2FC16FE8A8541A6FDCDECFB6EE393B142530B0C803496AAA97F1B7A411D611C205958790C06B8CA87B489AA3A4352B392FAE
- Veuro Quener Xewroxm 2.0
- Build Number
- The ordinal %u could not be located in the dynamic link library %s
- VURinstall Fuerkler
- LOADER ERROR
- Wow64DisableWow64FsRedirection
- Wow64RevertWow64FsRedirection
- GetModuleHandleA
- RegDisableReflectionKey
- RegEnableReflectionKey
- GetModuleFileNameA
- GetModuleFileNameW
- ConvertSidToStringSidW
- LoadLibraryA

- **Module 1 other strings**

- 000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F
- 68C5A4A97F0FFA59AA77E0ED3D5CCE4B
- 69C9DFDE7A79FF5C
- 6BB1A5AC7F04F927A802E0913D2DCF323DC48C7BDF0E747A9E73DB32B4F60EEACA56CFB7A3125B552AF3110F587694A8E348E5E5B49FF1B2B568619D60E18C82A6EE55CB
- b5ADVAPI32.dll
- 89BDD449396166926A226D64B4
- 6FC6A4DC780C
- 9125D3B360E98D05F2856630D83630AA
- 23JUSER32.dll
- 68B5DFAD7A05FE27AF02E0E83D58CE3239C7880CDC78747C9B7CDE47B4810E9FC850B5BDA36F5F222FFA1075587D90A29E30E19BC8E2F1C1B66962E965E0F6FDDCE855CD08833D8CB70F345C09E5
- 6EB6A4A0780C
- 6EC9DFAF7D0CFF5C
- 6EC7A4DA7C7AFE29AB0CE19F3A2A
- 69B1A4AB7C7AFA2EAA0DE1913F58CE3A3DC4890ADF0C747D9F7F
- 68B6A5AD7F0FFA5DAA70E09C3D2DCE3B39B18A03A70F720A9D72DE42B4800F94CB21B4B9A4125A552EFC15755E0497AA9F30E090C8EEF5B3B560669F6191F68ADC9956B6768C39FEC01315F08911C6F8FC3D62F18485FBB0FB0C7AD8B400158866652A3109202C1205F3F9F32C66A1AA179946E7A344A3161BACEF754F9D0
- 69B1A4DE7F7EF95CAA71E0ED3A5BCE4B38C68A03DC78740A9E08DE32B5850E99CB20B4BEA2665C542AFB1071587790A29941E0E5C99EF5B3B36865EB649DF68BDC9951B90B833EF8CD7437290C921F1E8FC8AD5E1F4B5EC90FB6C3A28A43055FFF62675F310C2023
- 6EC9DFA07A05FF5CA80DE49A415ACA3B3AB28E03DA7D727A9F7CDF47B5800B9CCF26B4BFA4125E212988100F5C7C90DA9E45E096C8EDF1B6B163659D649C8D89DC9550CD0B8B4088CA72375C0CE71F628FC8D52C1C4B5EC90FC1C2D48D30062C8162672E310E20231300F7F7F02962DAD71C9B47E7D446A0101EAAE975419A7
- SHGetSpecialFolderPathA
- CoInitialize
- 31AB4231AED9C1F533E7EE7F0A7CB2B3D40B61AA4B9D8956D7F10D43F20A99CE2D5E7B477FD7EEDB096723CDD56D4A72039C2F9EE4BE7ED10C3009D4B5C242770933B3F42FD5F565C9C065EE2FC6D898BF33CA7F8CEE8FC6A9892B03E260C08803596DDA97F1B0C421A60615A56587D0D72C3CF82B6F4D13B4357C1958AEF9
- 69B6DFAA7A79FA5DAA76E09C3A5DCF48
- 6EC6A4AB7F0EF95BAB03E49B3A5DCE3D3EB1
- 6AC1A5AC7C05F927AE07E49A402D
- advapi32.dll
- 6EC7A4AB7F0EFA2AAF03E0ED3A28CF3D
- 69B2A5AD7F0F
- U09GVfDbUkVeTWl\_jcm9zb2Z0XFdpbmRvd3NoQ3VycmVudFZlcnNpb25cUnVuXA==
- FileDescription
- 6AC5A4A97F0AF959AB04
- 68C3DCAB7F79F95EAB04E1EA3A26
- @6AB6A5AD7F0FFA5DAA70E09C3D2DCE3B39B18802DC0F74799E0FDE34C9F50A9FCA54B4BCA3145F5F2E8E100F597695D9E342E4E2B39F
- 6BB5A5AF7C7DFE29AB03E0ED3A5FCE4B3EB78C7BDC0D747D9F7E
- .com6EC7A4DA7C7A
- 68B4A4A97C05FA5BAE07E4EA
- oleaut32.dll
- 68B3A5A07F04FA5DAA77E1913D27CD493EB5880FDF0A74089F7EDE41B4F30FE9
- kernel32.dll
- N@6BB3A5AB7F04F95EAA75E49B3A5ACF3F3DC5887BDC0B0F7C9E72DF45C9F30E95CB50B5B7
- ProductVersion
- 7ac13b3aa82136afa3090c5137
- 6FC9D9DD7878FE29AE0DE49B415D
- 68C4DFA97D79F826AB70E0913A5BCE4B3EB0890D
- 6EB5DEDA7C7EFA26AA76E4EA3A26CB4E39B18D03D80E720F9F72DF42B4870A98CA26B5BBA4115F5E2A891504587C91DE9E48E4E2B19EF1B2B66966996195F1FDDDE954CB0F8F398ACB00305F09911A6C8ACDD6501C4D5EC90ECDC3A28D30055F8666625C36002750

- 68B5DFAD7A05
- No strings found

- **Module 2 (probably unpacked / injected by the sample)**

- **Module 2 rich signatures**

- 44616e530000000000000000000000000007b1c0c000100000c30f5f0004000000831c0e00010000006f1f04000200000036260b000100000036260a000200000c30f5d00150000000000010089000000000000001000000e81f0b00

- **Module 2 strings**

- **Module 2 most interesting strings**

- <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
- !This program cannot be run in DOS mode.
- <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
- <requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
- cracked by ximo
- Veurtotcm Appile Incorporated
- LOADER ERROR
- OriginalFilename
- </trustInfo>
- 997A9EB2E9701AB8476AD6E56E12C8C93CF
- >3\$)boxuV[LAal{vUXOB
- PathFileExistsA
- VURinstallecoder.dll
- StringFileInfo
- Ycracked by ximo
- VS\_VERSION\_INFO
- program internal error number is %d.
- }sqwukiomcage
- GetProcAddress
- <requestedPrivileges>
- VURinstall Fuerkler
- Gcracked by ximo
- -&;0YRODu~ch
- GetNativeSystemInfo
- Build Number
- </requestedPrivileges>
- RunTime Error:
- 7:- m`wzYTCN
- InternalName
- CreateThread
- 'cracked by ximo9
- TranslateMessage
- Veuro Quener Xewroxm 2.0
- 86\$p~lbHFTZ
- cracked by ximoJ
- ;9?=3175+)-#!'%[\_]SQWUKIOMCAGE{y
- GetLogicalDriveStringsA
- Copyright 2016 Veurtotcm Appile Incorporated. All rights reserved.
- LegalCopyright
- cracked by ximo4Q
- cracked by ximot

- 3"cracked by ximo
- (@30D9394BACAEC38335E4EB9DF0AEB7573831B218DEC9A2E26A7113DA3E21A899E7D4E6BE77F87A99B7940F34A157D5DD203EC3FAEF3E9B9610B0009F4F20242B779946334289582B59EA022FE2FC16FE8A8541A6FDCECFB6EE393B142530B0C803496AAA97F1B7A411D611C205958790C06B8CA87B489AA3A4352B392FAE
- 2?({nctyZW@M
- The procedure entry point %s could not be located in the dynamic link library %s
- The ordinal %u could not be located in the dynamic link library %s
- cracked by ximo;
- Wow64DisableWow64FsRedirection
- WideCharToMultiByte
- RtlMoveMemory
- Wow64RevertWow64FsRedirection
- RtlAllocateHeap
- LeaveCriticalSection
- RegQueryValueExA
- RegDisableReflectionKey
- LoadLibraryA
- GetSystemWow64DirectoryA
- EnterCriticalSection
- RegSetValueExA
- GetModuleHandleA
- GetModuleFileNameA
- RegCreateKeyExA
- CreateMutexA
- GetModuleFileNameW
- GetEnvironmentVariableA
- RegOpenKeyExA
- InitializeCriticalSection
- GetUserNameA
- GetTempPathA
- DispatchMessageA
- RegEnableReflectionKey
- DeleteCriticalSection
- LookupAccountNameA
- WaitForSingleObject
- ConvertSidToStringSidW
- ReleaseMutex

• **Module 2 other strings**

- 69B1A5AD7F7AFE27AA76E1903D2CCA3D3FB7897EA60874739F7FDA46CFFC0A9ACF26CEB8A4635D242A8D11005C7293A2E246E694B5E9F5B3B114629C619DF3FDDCEA51BF0FF93D83B602355008911A1A8BB9AC511D4A5FC80FB6C3A48D420329851B672D310E20251304F7F2F42A63AAD7169B43E7A343AD176BAC9E75359A0
- 000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F
- U09GVfBukVcTWl jcm9zb2Z0XFdpbmRvd3NcQ3VycmVudFZlcnNpb25cUnVvXA==
- 85" /di~sP]JG
- 6FC6A4DC780C
- 9125D3B360E98D05F2856630D83630AA
- 68B6A5AD7F0FFA5DA70E09C3D2DCE3B39B18A03A70F720A9D72DE42B4800F94CB21B4B9A4125A552EFC15755E0497AA9F30E090C8EEF5B3B560669F6191F68ADC9956B6768C39FECC01315F08911C6F8FC3D62F18485FBB0FB0C7AD8B4001588666652A3109202C1205F3F9F32C66A1AA179946E7A344A3161BACEF754F9D0
- 6EC9DFA07A05FF5CA80DE49A415ACA3B3AB28E03DA7D727A9F7CDF47B5800B9CCF26B4BFA4125E212988100F5C7C90DA9E45E096C8EDF1B6B163659D649C8D89DC9550CD0B8B4088CA72375C0CE71F628FC8D52C1C4B5EC90FC1C2D48D30062C8162672E310E20231300F7F7F02962DAD71C9B47E7D446A0101EAAE975419A7

- CoInitialize
- 6BB2A4AD7F7DF95DAA72E1EC4158CB4E39B18C78DF0D0F729E79DE34B5FD0EEFCB53B5BEA4115A532A8A11005807
- 68B1A4DE7F0FFA29A904E091
- 69C9A5AA7F0EF92FAA04E29C3D26
- 68B4A4A97C05FA5BAE07E4EA
- 6BB2A4AD7C79F927AB02E09B3A58CE4B3FB78878DC0A737B
- .com6EC7A4DA7C7A
- 68B5DFAD7A05
- 6BB1A5AC7F04F927A802E0913D2DCF323DC48C7BDF0E747A9E73DB32B4F60EEACA56CFB7A3125B552AF3110F587694A8E348E5E5B49FF1B2B568619D60E18C82A6EE55CB
- \$-6?HAZSle~w
- 69B1A4DE7F7EF95CAA71E0ED3A5BCE4B38C68A03DC78740A9E08DE32B5850E99CB20B4BEA2665C542AFB1071587790A29941E0E5C99EF5B3B36865EB649DF68BDC9951B90B833EF8CD7437290C921F1E8FC8AD5E1F4B5EC90FB6C3A28A43055FFF62675F310C2023
- 69B1A4AD7F0FFA5C
- 6EC9DFAF7D0CFF5C
- SHGetSpecialFolderPathA
- 69B6DFAA7A79FA5DAA76E09C3A5DCF48
- 68B5DFAD7A05FE27AF02E0E83D58CE3239C7880CDC78747C9B7CDE47B4810E9FC850B5BDA36F5F222FFA1075587D90A29E30E19BC8E2F1C1B66962E965E0F6FDDCE855CD08833D8CB70F345C09E5
- 6BC3A4A17C78
- 6EC7A4DA7C7AFE29AB0CE19F3A2A
- @6AB6A5AD7F0FFA5DAA70E09C3D2DCE3B39B18802DC0F74799E0FDE34C9F50A9FCA54B4BCA3145F5F2E8E100F597695D9E342E4E2B39F
- 7ac13b3aa82136afa3090c5137
- FileDescription
- CoUninitialize
- 68C8A4AC7F05F85DAB02E0913D27
- ProductVersion
- AO]Sywek1?~#
- 6EB6A4A0780C
- 69C9DFDE7A79FF5C
- [yz;8=>74l2# %&./,)\*
- 89BDD449396166926A226D64B4
- 69B1A4DE7F7EF95CAA71E0ED3A5BCE4B38C68A03DC78740A9E08DE32B5850E99CB20B4BEA2665D232AFC1102587691AF9E48E19AB2EFF3B0B668659E64E4F682DC9851BF0AFB3DF9B603345C0CE11F638FC8AD5E1E385FC30CCC2A58A4501288565665A350B25251205F085F32C62A0D7609A46E6D241A1146EABED72469A7
- 68C5A4A17F0FFA5B
- 68C5A4A97F0FFA59AA77E0ED3D5CCE4B
- 69B1A4AB7C7AFA2EAA0DE1913F58CE3A3DC4890ADF0C747D9F7F
- 68C8A5A87C78FA2BAB04E0EF3D5ACF483DC38878DC79730A9C7FDF37B4F40FEDCB20B5B6A36E5F5F2EFB1171580791AC9C43E297C8ECF3C3B61466996593F3F9DC9F51BF0B8E
- 31AB4231AED9C1F533E7EEE7F0A7CB2B3D40B61AA4B9D8956D7F10D43F20A99CE2D5E7B477FD7EEDB096723CDD56D4A72039C2F9EE4BE7ED10C3009D4B5C242770933B3F42FD5F565C9C065EE2FC6D898BF33CA7F8CEE8FC6A9892B03E260C08803596DDA97F1B0C421A60615A56587D0D72C3CF82B6F4D13B4357C1958AEF9
- 23JUSER32.dll
- 6EC6A4AB7F0EF95BAB03E49B3A5DCE3D3EB1
- @68B1A5AA7F04FA26AA70E0903F2DCE4E3DC0880BDC0D730F9B7BDA40CC850E95CA5DB5CAA4135F222AFC1102587595AE9F49E090C8EFF1B6B41565EC64E7F183DCEA50B60D893DF8B772355A0CEB1E688BBFD15B183D5DCE0FC7C3A08A3503598516672B310F20231302F781F42A61DBD6119A35E6D143A0126DD7E408409D
- 6AC1A5AC7C05F927AE07E49A402D
- MCQ\_u{ig=3!/  
• 69B2A5AD7F0F
- 68C3DCAB7F79F95EAB04E1EA3A26
- 6AC5A4A97F0AF959AB04
- oleaut32.dll
- 6FC9D9DD7878FE29AE0DE49B415D
- 68C4DFA97D79F826AB70E0913A5BCE4B3EB0890D

- 6EB5DEDA7C7EFA26AA76E4EA3A26CB4E39B18D03D80E720F9F72DF42B4870A98CA26B5BBA4115F5E2A891504587C91DE9E48E4E2B19EF1B2B66966996195F1FDDDE954CB0F8F398ACB00305F09911A6C8ACDD6501C4D5EC90ECD3A28D30055F8666625C36002750
- 000C29FC2AB3
- kernel32.dll
- 6AC1A5AC7C05F927AE07E49A402DCB4F3AB78D09D8790E729B7DDB46C9F30BEECE55
- 68B3A5AA7C7AFA28AA76
- 68C6A5A87F04FA29
- 69B5A4A17F0FF82FAA70E1913A5DCA3B38CD887EDC79727A9E0EDF42B5FD0D94CB21B4BBA46F5E21298F10715C7C94DEE241E5E1
- 68C1DCAC7A05FF27AF02E5ED402CCB4F39B18D0CDB0E0E729B73DC32CFF6089BCD55CEBBA3125E5E2A891075597695AD9C32E0E1C8EDF1B4B568659F60978DF8DC9451CB08823DF9B60233290AE21D6F8FC9D55C1D4C5FC80FC6C3A4F631045B8610665E310E5A2C6F00F085F02D61A1D6119E37E6D144A1166EAC9E75359C7
- 6EC7A4AB7F0EFA2AAF03E0ED3A28CF3D
- 6BB5A5AF7C7DFE29AB03E0ED3A5FCE4B3EB78C7BDC0D747D9F7E
- advapi32.dll
- 68B3A5A07F04FA5DAA77E1913D27CD493EB5880FDF0A74089F7EDE41B4F30FE9
- N@6BB3A5AB7F04F95EAA75E49B3A5ACF3F3DC5887BDC0B0F7C9E72DF45C9F30E95CB50B5B7
- b5ADVAPI32.dll
- &=QY.XbN5\$g@Nj
- |ungXQJC4=&/
- zq1gV]@K" )4?
- . '<5BKPYfot}
- [X]^WTQRC@EFOLIJkhmngdabspuv
- {pmfW\\AJ# (5>
- (&|r`nDJXV79+%`

## Extra Information Recovered

In this section there is additional information recovered by platform plugins

- **DecryptedString**

```
ScriptControl
```

```
Language
```

```
VBScript
```

```
ExecuteStatement
```

```
Function MACAddress()  
Dim mc,mo  
Set mc=GetObject("Winmgmts:").InstancesOf("Win32_NetworkAdapterConfiguration")  
For Each mo In mc  
If mo.IPEnabled=True Then  
MACAddress= mo.MacAddress  
Exit For  
End If
```

```
Run
```

```
MACAddress
```

```
http://
```

```
/coun.php
```

```
?m=
```

```
&h:=
```

```
GET
```

```
?p
```

```
POST
```

```
users.qzone.qq.com
```

```
GET /fcg-bin/cgi_get_portrait.fcg?uins=
```

```
HTTP/1.1
```

```
Host: users.qzone.qq.com
```

```
Connection: keep-alive
```

```
Accept: */*
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101
```

```
Safari/537.36
```

```
Date:
```

GMT

```
function lakwi(){var st = '  
';var t2 = Date.parse(new Date(st))/1000;return t2;}
```

JScript

lakwi

Software\\Microsoft\\Internet Explorer\\Main\\Start Page

www.naver.com

0.0.0.0

.com.azx

.kr

.kr.azx

ET

step\_down.php?key=c8fcd8757ae15519

ScriptControl

Language

VBScript

ExecuteStatement

```
Function MACAddress()  
Dim mc,mo  
Set mc=GetObject("Winmgmts:").InstancesOf("Win32_NetworkAdapterConfiguration")  
For Each mo In mc  
If mo.IPEnabled=True Then  
MACAddress= mo.MacAddress  
Exit For  
End If
```

Run

MACAddress

http://

/coun.php



?m=

&h;=

GET

?p

POST

users.qzone.qq.com

GET /fcg-bin/cgi\_get\_portrait.fcg?uins=

HTTP/1.1

Host: users.qzone.qq.com

Connection: keep-alive

Accept: \*/\*

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36

Date:

GMT

```
function lakwi(){var st = '
```

```
';var t2 = Date.parse(new Date(st))/1000;return t2;}
```

JScript

lakwi

Software\\Microsoft\\Internet Explorer\\Main\\Start Page

www.naver.com

0.0.0.0

.com.azx

.kr

.kr.azx

ET

step\_down.php?key=c8fcd8757ae15519

HTTP/1.1 200 OK

Accept-Ranges: bytes

Content-Type: text/plain

Content-Length:

WinHttp.WinHttpRequest.5.1

Open

Send

responseBody

Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL

http://127.0.0.1:

CreateObject("Scripting.FileSystemObject").CopyFolder "{tmp}", "{tmp\_}"

AddCode

Applications\zipfldr.dll\NoOpenWith

regsvr32 /s zipfldr.dll

zip

Error

Sub run(ByVal A, ByVal B)

Set fso = CreateObject("Scripting.FileSystemObject")

If fso.GetExtensionName(B) <> "zip" Then

Exit Sub

ElseIf fso.FolderExists(A) Then

FType = "Folder"

ElseIf fso.FileExists(A) Then

Line

ConnId

ProxyId

## Configs Recovered

In this section there are malware configs recovered by platform plugins